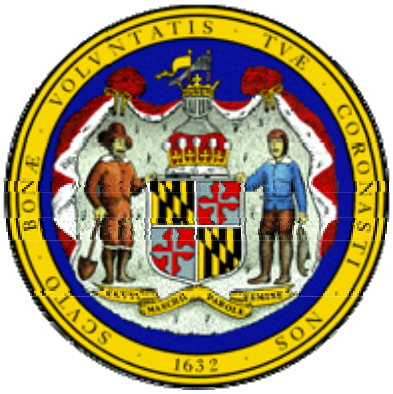

State of Maryland

State of Maryland

Department of Budget and Management

Statewide Security Support

MD-Computer Incident Response Capability Procedures

September 2005

MD-CIRC Users Guide
Information Security Incident Procedures

In the event you have, or think you have an Information Security Incident:

- Do **NOT** Panic.

- Do **NOT** Investigate the system to see what happened
  - ***Do NOT*** *Log-in to the system*
  - ***Under NO*** *Circumstances should you log-in with ROOT access.*

- **Do** Contact the MD-CIRC.

  By Phone:

  410-260-7778

  Via E-mail:

  ircmaryland@dbm.state.md.us

  By Fax:

  410-974-5060

The following pages will provide basic information to guide you through the Security Incident process.

An Incident Response Service Overview

Overview
Maryland's Incident Response service will provide Maryland agencies with a central location for incident reporting and tracking which will allow the State's decision makers to proceed with accurate information about security incidents as they occur, and about trends in information security. Users of the service will receive up to date, relevant steps to help them mitigate their problems.

1. Incident Reporting Format.

The following is an Incident Information Sheet that can be filled out and faxed to the MD-CIRC in the event of an incident. If you are communicating with the MD-CIRC via E-mail, fill the information out and paste it into the body of the your e-mail. In the event that you are reporting via phone, the Incident Analyst will ask you for this information. Do not hold up the reporting process trying to find out all the below information prior to calling – gather what information you can quickly and make the call.

You may not be able to answer all the questions at the time of an incident. Those fields that require an answer at the time of incident reporting are indicated in **BOLD.**

1.1. Your Agency, Department or Board?

1.2. Your Name?

1.3. Point of Contact for handling the incident?

1.4. How should the MD-CIRC reply to your POC? Provide contact information, i.e. phone number or e-mail address.

1.5. How soon do you need a reply to your report? (ASAP, next business day, within the week.)

1.6. Incident Type i.e. what happened? Incidents are categorized as:

Increased access
Disclosure of information
Corruption of information
Denial of service
Theft of resources
Non-incident

1.7. **Was the attempt successful?** Yes No

1.8. Is the incident ongoing? Or, is it over?

1.9. What was the severity of the incident (see incident severity questionnaire)?

1.10. Do you have an agency tracking number associated with this incident? Yes No
What is the number?

1.11. Is there any other tracking number associated with this incident? Yes No
What is the number?

1.12. What was the date of the incident? MM/DD/YYYY

1.13. What was the local time of the incident? HH:MM (please use 24 hour GMT Format.)

1.14. Where is (are) the effected system (s) located?

1.15. **IF KNOWN, what is the related vulnerability**? (The *vulnerability* is the flaw or bug being exploited, e.g., IIS Unicode, MSSQL Null password, etc.)

1.16. IF KNOWN, what is the related tool? (The *tool* is the software that is exploiting the vulnerability, e.g., Code Red, Worm, Virus, etc.)

1.17. How was the incident detected?

1.18. What, if anything, has been done so far to mitigate?

1.19. Do you suspect criminal activity?

1.20. Have you reported the incident to law enforcement?

1.21. Have you reported the incident to anyone else?

TARGET or affected system (s)

1.22. What is the IP address of the affected system (s)?

1.23. **What is the operating system (OS) of the affected system**?

1.24. What is the primary function of this system?

1.25. What is the port number or service that was affected?

ATTACKER or source system (s)

1.26. Is the Incident Source internal or external to your organization?
Is it FOREIGN?

1.27. Is the attacking IP address known?
What is it?

SHARING means sharing DETAILED incident information, including the affected agency. Permission to share sanitized incident information is assumed and implicit, regardless of the responses below.

1.28. Share with Maryland State Police (MSP)? Y N

1.29. Share with Maryland Emergency Management Agency (MEMA)? Y N

1.30. Share with National Infrastructure Protection Center (NIPC)? Y N

1.31. Share with CERT Coordination Center at Carnegie Mellon University? Y N

1.32. Share with United States Computer Emergency Readiness Team (US-CERT)? Y N

1.33.	Share with US Department of Defense CERT (DoD-CIRC)?	Y	N
1.34.	Share with another Maryland State Agency?	Y	N
1.35	Share with Multi-State Information Sharing Analysis Center?	Y	N

Incident Severity Questionnaire

The Incident Severity is a numerical value representing the impact of a particular incident. This numerical value is based on the answers to the questions below. Formal models such as this are subject to errors, especially when presented with unusual or unexpected input. Users should review the resulting numerical Incident Severity value for appropriateness before finalizing the submission; users may elect to assign a different Incident Severity value. An Incident Severity explanation field is available for any relevant comments.

The Incident Severity determination is a point-based system. Answer the questions below; sum the points to obtain an Incident Severity value, including a list of the increasing and decreasing factors. The resulting value will be 0-10. Certain questions override the others and result in an absolute Incident Severity value (noted by IS = #); the Incident Severity determination process can be terminated at this point (if an absolute Incident Severity value is indicated). The other point values are of the form +/- #. Unknown or not applicable questions should be scored as 0 points.

The results of this model should be input to the report above, but this questionnaire can also be sent via fax or e-mail to the MD-CRC

Minimum Value: - 4

Maximum Value: + 10

Q1. Is the incident report purely informational, i.e., no incident occurred?

A1. YES: IS=0
NO: +0

Q2. How many systems are/were affected by the incident?

A2. 1: +0
2-10: +1
10 or more: +2

Q3. What is the criticality of the affected system(s)?

A3. LOW: +0 (minimal operational impact)
MEDIUM: +1 (moderate operational impact)
HIGH: +2 (mission critical systems)

Q4. Is a fix available for the exploited vulnerability?

A4. PERMANENT FIX AVAILABLE FOR MORE THAN 1 WEEK: +0
PERMANENT FIX AVAILABLE FOR LESS THAN 1 WEEK or WORKAROUND ONLY, NO PERMANENT FIX AVAILABLE: +1
NO WORKAROUND OR FIX AVAILABLE: +2

Q5. What was the effect of the incident?

A5. DENIAL OF SERVICE: +0
USER ACCOUNT COMPROMISE or UNAUTHORIZED ACCESS TO INFORMATION: +1
ROOT OR ADMINISTRATOR LEVEL COMPROMISE: +2

Q6. Was the attacker internal or external?
A6. INTERNAL: +0
EXTERNAL: +1

Q7. Can action be taken immediately to mitigate the ongoing risk?
A7. NO: +0
YES: +1

Q8. Is the affected application or platform in widespread use at other sites (i.e., within the affected organization or without)?
A8. ONLY USED AT THIS SITE: -2
MINIMAL USE ELSEWHERE: -1
WIDESPREAD DEPLOYMENT AND USAGE: +0

Q9. What level of skill and prerequisites are required by the attacker to perpetrate the attack?
A9. HIGHLY SKILLED ATTACKER and/or MULTIPLE PREREQUISITES: -2
MODERATE SKILL and/or SOME PREREQUISITES: -1
MINIMAL SKILL or MINIMAL/NO PREREQUISITES: +0

Incident Severity (Total Points) = _____